A resultant formula for Hensel's Lemma

Juliane Deißler

January 18, 2013

Let R be a complete discrete valuation ring with maximal ideal generated by π. Let $f(X) \in R[X]$ be a monic polynomial. Suppose given a factorisation of $f(X)$ modulo π^s into several factors. Under certain assumptions we lift it to a true factorisation of $f(X)$ in $R[X]$. This generalises the Hensel-Rychlík Lemma, which covers the case of two factors. We work directly with lifts of factorisations into several factors and avoid having to iterate factorisations into two factors. For this purpose we define a resultant for several polynomials in one variable as a determinant of a certain matrix.

Contents

0 Introduction

In this introduction, by a polynomial we understand a monic polynomial.

0.1 Resultant of several polynomials

Let S be an integral domain. We define the resultant of several polynomials in $S[X]$, analogously to the resultant of two polynomials, as a determinant of a certain matrix; cf. van der Waerden, [**6,** §34]. For n polynomials $g_{(1)}(X), \ldots, g_{(n)}(X) \in S[X]$, $n \geq 1$, the resultant $\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})$ is given by the determinant of the matrix $A(g_{(1)}, \ldots, g_{(n)})$ whose entries are coefficients of products of the polynomials $g_{(1)}(X), \ldots, g_{(n)}(X)$ that omit respectively one of them; cf. Definition 1.

MSC2010: 13B25.

Consider the polynomials $g_{(1)}(X), \ldots, g_{(n)}(X)$ as having coefficients in a large enough field. Write $g_{(k)}(X) =: \prod_{i \in [1, \deg g_{(k)}]} (X - \gamma_{(k)i})$ for $k \in [1, n]$. In Lemma 2 we state that $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) = \prod_{1 \leq k < \ell \leq n} \ \prod_{(i,j) \in [1, \deg g_{(k)}] \times [1, \deg g_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j})$.

In particular, we have $\operatorname{Res}(g_{(1)} , \ldots , g_{(n)}) = \prod_{1 \leq k < \ell \leq n} \operatorname{Res}(g_{(k)} , g_{(\ell)})$. Since in our application below the matrix $A(g_{(1)}, \ldots, g_{(n)})$ is used in a crucial way, it would not have been possible to work just with the right hand side of this equation.

0.2 Applications to Hensel's Lemma

Let R be a complete discrete valuation ring and $\pi \in R$ a generator of its maximal ideal.

0.2.1 General case

Hensel's Lemma in its classical form can, in rudimentary form, already be found in [**3,** §374]; cf. [**2,** §3.6]. Hensel [**4,** §4, p. 80] developed a more sophisticated version, known today as Hensel-Rychlík Lemma. We generalise in Theorem 12 the Hensel-Rychlík Lemma from the case of two factors to the case of an arbitrary number of factors.

Let $n \geq 1$ and $f(X)$, $g_{(1)}(X)$, $\ldots$, $g_{(n)}(X) \in R[X]$ of degree ≥ 1 be such that $f(X) \equiv_{\pi^s} \prod_{k \in [1,n]} g_{(k)}(X)$ for some $s \geq 2t + 1$, where $t := \mathrm{v}_\pi(\operatorname{Res}(g_{(1)} , \ldots , g_{(n)}))$. Then there exist polynomials $\check{g}_{(1)}(X)$, $\ldots$, $\check{g}_{(n)}(X)$ in $R[X]$ congruent, respectively, to $g_{(1)}(X)$, $\ldots$, $g_{(n)}(X)$ modulo π^{s-t} such that $f(X) = \prod_{k \in [1,n]} \check{g}_{(k)}(X)$. In addition, the polynomials $\check{g}_{(1)}(X)$, $\ldots$, $\check{g}_{(n)}(X)$ are unique.

Lemma 11 contains the main part of the proof of Theorem 12. The arguments for that I have learnt from Koch, [**5,** 4.4.3, 4.4.4, 4.4.5].

In Example 14 we assume that $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ to compare the result of a single application of Lemma 11 to three factors with the result of two subsequent applications of Lemma 11 to two factors. We determine that both methods are essentially equally good.

0.2.2 Particular case $f(X) \equiv_\pi X^M$

In § 2.3 we investigate our generalisation of the Hensel-Rychlík Lemma in a particular case. Let $f(X)$ be a polynomial in $R[X]$ with $\deg f =: M$ and $f(X) \equiv_\pi X^M$. Let $n \geq 1$ and $g_{(1)}(X)$, $\ldots$, $g_{(n)}(X) \in R[X]$ of degree ≥ 1 ordered such that $\deg g_{(1)} \leq \cdots \leq \deg g_{(n)}$. Again, we write $t := \mathrm{v}_\pi(\operatorname{Res}(g_{(1)} , \ldots , g_{(n)}))$. Moreover, we write $t' := t - \sum_{j \in [1, n-1]} \big((n-j) \deg g_{(j)} - 1\big)$. Now, suppose that $f(X) \equiv_{\pi^s} \prod_{k \in [1,n]} g_{(k)}(X)$ for some $s \geq t + t' + 1$. Then there exist polynomials $\check{g}_{(1)}(X)$, $\ldots$, $\check{g}_{(n)}(X) \in R[X]$ congruent, respectively, to $g_{(1)}(X)$, $\ldots$, $g_{(n)}(X)$ modulo $\pi^{s-t'}$ such that $f(X) = \prod_{k \in [1,n]} \check{g}_{(k)}(X)$. In addition, the polynomials $\check{g}_{(1)}(X)$, $\ldots$, $\check{g}_{(n)}(X)$ are unique. Cf. Theorem 18.

The proof of Theorem 18 is similar to the respective proof in the general case. We refrained from attempting to produce an assertion that covers both the general Theorem 12 and the more particular Theorem 18, for it probably would have obscured Theorem 12.

Lemma 17 contains the main part of the proof of Theorem 18. In Example 19, we assume that

$f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$, where $\deg g_{(1)} \le \deg g_{(2)} \le \deg g_{(3)}$, to compare the result of a single application of Lemma 17 to three factors with the result of two subsequent applications of Lemma 17 to two factors. Under the present hypothesis $f(X) \equiv_\pi X^M$, we determine that the former method yields a somewhat more precise result than the latter method.

To illustrate the theory we consider in § 3 some polynomials with cofficients in $\mathbb{Z}_p$ for a prime number p using the computer algebra system MAGMA [**1**].

0.3 Notations

- Given $a,\, b \in \mathbb{Z}$, we denote by $[a,b] := \{z \in \mathbb{Z} \,:\, a \le z \le b\} \subseteq \mathbb{Z}$ the integral interval.
- Given an integral domain R, a prime element $\pi \in R$ with $\pi \neq 0$ and $x \in R \smallsetminus \{0\}$, we denote $\mathrm{v}_\pi(x) := \max\{\, i \in \mathbb{Z}_{\ge 0} \,:\, \pi^i \text{ divides } x \,\}$.

1 Resultants

Let R be an integral domain. Let $\pi \neq 0$ be a prime element of R. Let $n \in \mathbb{Z}_{\ge 1}$. Suppose given monic polynomials $g_{(k)} = g_{(k)}(X) = \sum\limits_{i \in [0,m_{(k)}]} g_{(k)i} X^i \in R[X]$, where $m_{(k)} := \deg g_{(k)} \ge 1$, for $k \in [1,n]$. Denote $M := \sum\limits_{j\in[1,n]} m_{(j)}$. Denote $M_{(k)} := M - m_{(k)}$ and $\prod\limits_{j \in [1,n] \smallsetminus \{k\}} g_{(j)}(X) =: \sum\limits_{i \in [0, M_{(k)}]} a_{(k)i} X^i$ for $k \in [1,n]$.

Let K be the field of fractions of R. Let L be a splitting field for $\prod_{k\in[1,n]} g_{(k)}(X) \in K[X]$. Write

$$A(g_{(1)},\dots,g_{(n)}) \;:=\; \left(\begin{array}{ccccccc}
a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} \\
a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}}
\end{array}\right)
\begin{array}{l}
\left.\begin{array}{c}\vphantom{a}\\ \vphantom{a}\\ \vphantom{a}\end{array}\right\} m_{(1)}\text{ rows} \\
\left.\begin{array}{c}\vphantom{a}\\ \vphantom{a}\\ \vphantom{a}\end{array}\right\} m_{(2)}\text{ rows} \\
\vphantom{\vdots} \\
\vphantom{\vdots} \\
\left.\begin{array}{c}\vphantom{a}\\ \vphantom{a}\\ \vphantom{a}\end{array}\right\} m_{(n)}\text{ rows}
\end{array}
\;\in\; R^{M\times M}\,.$$

Definition 1. Let

$$\mathrm{Res}(g_{(1)},\dots,g_{(n)}) \;:=\; \det A(g_{(1)},\dots,g_{(n)}) \;\in\; R$$

be the *resultant* of $g_{(1)}(X)\,,\dots,\, g_{(n)}(X)$.

Lemma 2. *Write* $g_{(k)}(X) \;=:\; \prod\limits_{i\in[1,m_{(k)}]} (X - \gamma_{(k)i})$ *in* $L[X]$ *for* $k \in [1,n]$.

We have

$$\operatorname{Res}(g_{(1)},\ldots,g_{(n)}) \;=\; \prod_{1\le k<\ell\le n}\;\prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (\gamma_{(k)i}\,-\,\gamma_{(\ell)j})\;.$$

This generalises the well-known assertion in the case $n=2$; cf. e.g. [**6,** §35].

Proof. Write $m^{(k)} := \sum_{\ell\in[1,k]} m_{(\ell)}$ and $I^{(k)} := [1,m^{(k)}]$ for $k\in[0,n]$.
Write $I_{(k)} := [m^{(k-1)}+1,m^{(k)}]$ for $k\in[1,n]$.

Step 0. Let $\hat{L} \;:=\; K[\underbrace{\hat{\gamma}_{(1)1}\,,\,\ldots\,,\,\hat{\gamma}_{(1)m_{(1)}}}\,,\underbrace{\hat{\gamma}_{(2)1}\,,\,\ldots\,,\,\hat{\gamma}_{(2)m_{(2)}}}\,,\;\ldots\ldots\;,\underbrace{\hat{\gamma}_{(n)1}\,,\,\ldots\,,\,\hat{\gamma}_{(n)m_{(n)}}}]$ be a polynomial ring in M variables. Let F be its field of fractions. So $K\subseteq L$ and $K\subseteq\hat{L}\subseteq F$.
For $\ell\in[1,n]$, let $\hat{g}_{(\ell)} = \hat{g}_{(\ell)}(X) := \prod\limits_{i\in[1,m_{(\ell)}]}(X-\hat{\gamma}_{(\ell)i}) \in \hat{L}[X]$. For $k\in[1,n]$, denote $\prod\limits_{\ell\in[1,n]\smallsetminus\{k\}}\hat{g}_{(\ell)}(X) =: \sum\limits_{i\in[0,M_{(k)}]}\hat{a}_{(k)i}X^i$. Moreover, let $\hat{a}_{(k)i} := 0$ for $k\in[1,n]$ and $i\in\mathbb{Z}\smallsetminus[0,M_{(k)}]$.
Step 1. Suppose given $\kappa,\ \lambda\in[1,n]$ with $\kappa\neq\lambda$. Suppose given $\mu\in[1,m_{(\kappa)}]$ and $\nu\in[1,m_{(\lambda)}]$. Consider the K-algebra homomorphism $\Psi:\hat{L}[X]\to\hat{L}[X]$ that maps $\hat{\gamma}_{(\kappa)\mu}$ to $\hat{\gamma}_{(\lambda)\nu}$ and each other variable to itself.
Let $u(X) = \sum\limits_{i\in[0,m_{(\lambda)}-1]}u_iX^i := \prod\limits_{i\in[1,m_{(\lambda)}]\smallsetminus\{\nu\}}(X-\hat{\gamma}_{(\lambda)i})$. Let $v(X) = \sum\limits_{i\in[0,m_{(\kappa)}-1]}v_iX^i := \prod\limits_{i\in[1,m_{(\kappa)}]\smallsetminus\{\mu\}}(X-\hat{\gamma}_{(\kappa)i})$. We have

$$\text{(I)}\quad u(X)\cdot\Psi\big(\hat{g}_{(\kappa)}(X)\cdot\prod_{\ell\in[1,n]\smallsetminus\{\kappa,\lambda\}}\hat{g}_{(\ell)}(X)\big)\;-\;v(X)\cdot\Psi\big(\hat{g}_{(\lambda)}(X)\cdot\prod_{\ell\in[1,n]\smallsetminus\{\kappa,\lambda\}}\hat{g}_{(\ell)}(X)\big)\;=\;0.$$

Consider the coefficient in (I) that belongs to X^ι for $\iota\in[0,M-1]$. We have

$$\sum_{i\in[0,m_{(\lambda)}-1]}u_i\,\Psi(\hat{a}_{(\lambda)\iota-i})\;-\;\sum_{j\in[0,m_{(\kappa)}-1]}v_j\,\Psi(\hat{a}_{(\kappa)\iota-j})\;=\;0.$$

So we have the following matrix equation with entries in F.

$$(0\ldots0\;\underbrace{u_0\ldots u_{m_{(\lambda)}-1}}_{\text{region }\lambda}\;0\ldots0\;\underbrace{-v_0\cdots-v_{m_{(\kappa)}-1}}_{\text{region }\kappa}\;0\ldots0)\cdot A(\Psi(\hat{g}_{(1)})\,,\,\ldots\,,\,\Psi(\hat{g}_{(n)}))\;=\;0$$

Since $u(X)$ and $v(X)$ are monic, thus nonzero, it follows that

$$\Psi(\det A(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,)\,)\;=\;\det A(\Psi(\hat{g}_{(1)})\,,\,\ldots\,,\,\Psi(\hat{g}_{(n)}))\;=\;0.$$

Step 2. Maintain the elements $\kappa,\ \lambda\in[1,n]$, $\mu\in[1,m_{(\kappa)}]$ and $\nu\in[1,m_{(\lambda)}]$ from Step 1.
Consider the element $\det A(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,)$ of $\hat{L}$ as a polynomial in $\hat{\gamma}_{(\kappa)\mu}$, having coefficients in $K[\hat{\gamma}_{(1)1}\,,\,\ldots\,,\,\hat{\gamma}_{(\kappa-1)m_{(\kappa-1)}}\,,\,\hat{\gamma}_{(\kappa)1}\,,\,\ldots\,,\,\hat{\gamma}_{(\kappa)\mu-1}\,,\,\hat{\gamma}_{(\kappa)\mu+1}\,,\,\ldots\,,\,\hat{\gamma}_{(\kappa)m_{(\kappa)}}\,,\,\hat{\gamma}_{(\kappa+1)1}\,,\,\ldots\,,\,\hat{\gamma}_{(n)m_{(n)}}]$. By polynomial division, there exist polynomials $p=p(\hat{\gamma}_{(\kappa)\mu})$ and $q=q(\hat{\gamma}_{(\kappa)\mu})$ in $\hat{L}$ such that

$$\det A(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,)\;=\;(\hat{\gamma}_{(\kappa)\mu}\,-\,\hat{\gamma}_{(\lambda)\nu})\cdot p(\hat{\gamma}_{(\kappa)\mu})\;+\;q(\hat{\gamma}_{(\kappa)\mu})$$

and $\deg q(\hat{\gamma}_{(\kappa)\mu}) < \deg(\hat{\gamma}_{(\kappa)\mu}\,-\,\hat{\gamma}_{(\lambda)\nu}) = 1$. Thus

$$q\in K[\hat{\gamma}_{(1)1}\,,\,\ldots\,,\,\hat{\gamma}_{(\kappa-1)m_{(\kappa-1)}}\,,\,\hat{\gamma}_{(\kappa)1}\,,\,\ldots\,,\,\hat{\gamma}_{(\kappa)\mu-1}\,,\,\hat{\gamma}_{(\kappa)\mu+1}\,,\,\ldots\,,\,\hat{\gamma}_{(\kappa)m_{(\kappa)}}\,,\,\hat{\gamma}_{(\kappa+1)1}\,,\,\ldots\,,\,\hat{\gamma}_{(n)m_{(n)}}],$$

i.e. it is constant in $\hat{\gamma}_{(\kappa)\mu}$. In particular, $\Psi(q) = q$. Apply Ψ to the equation above.

$$\underbrace{\Psi(\det A(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,))}_{=0} \;=\; \underbrace{\Psi(\hat{\gamma}_{(\kappa)\mu} \,-\, \hat{\gamma}_{(\lambda)\nu})}_{=\hat{\gamma}_{(\lambda)\nu} - \hat{\gamma}_{(\lambda)\nu} = 0} \cdot \Psi(p(\hat{\gamma}_{(\kappa)\mu})) \,+\, \underbrace{\Psi(q)}_{=q}\,.$$

Hence $q \,=\, 0$. It follows that

$$\operatorname{Res}(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,) \;=\; \det A(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,) \;=\; (\hat{\gamma}_{(\kappa)\mu} \,-\, \hat{\gamma}_{(\lambda)\nu}) \cdot p(\hat{\gamma}_{(\kappa)\mu})\,.$$

Since κ, λ, μ and ν were chosen arbitrarily, we conclude that $\operatorname{Res}(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,)$ is divisible by $(\hat{\gamma}_{(k)i} \,-\, \hat{\gamma}_{(\ell)j})$ for $1 \le\, k \,<\, \ell \le n$ and $(i,j) \,\in\, [1, m_{(k)}] \times [1, m_{(\ell)}]$. So we obtain that

$$\operatorname{Res}_0(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}) \;:=\; \prod_{1\le k<\ell\le n} \;\; \prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]} (\hat{\gamma}_{(k)i} - \hat{\gamma}_{(\ell)j}) \quad \text{divides} \quad \operatorname{Res}(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}).$$

Step 3. We aim to show that $\operatorname{Res}_0(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}) = \operatorname{Res}(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)})$.
Step 3.1. Observe that $\operatorname{Res}_0(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)})$ is homogeneous of degree $\sum\limits_{1\le k<\ell\le n} m_{(k)}m_{(\ell)} \;=:\; d$. Since $\hat{a}_{(k)s}$ is the coefficient of X^s in $\prod\limits_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$, we have $\deg \hat{a}_{(k)s} \;=\; M_{(k)} - s$ for $s \in [0, M_{(k)}]$ and $k \in [1,n]$. Write $A(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,) \;=:\; (e_{s,t})_{s,t} \;\in\; \hat{L}^{M\times M}$.
We *claim* that each nonzero Leibniz-summand in the determinant $\det A(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,) \;=\; \operatorname{Res}(\,\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}\,)$ is homogeneous of degree d.
So consider one of them. Let $\tau \,\in\, \mathrm{S}_M$. We need to show that $e_{s,\tau(s)}$ is homogeneous and $\deg\big(\prod\limits_{s\in[1,M]} e_{s,\tau(s)}\big)$ equals d. If this Leibniz-summand is nonzero, then $e_{s,\tau(s)}$ is homogeneous of degree $\deg e_{s,\tau(s)} = \deg \hat{a}_{(k)\,\tau(s)-s+m^{(k-1)}} = M_{(k)} - \tau(s) + s - m^{(k-1)}$ for $s \in I_{(k)}$. Thus

$$\begin{aligned}
\deg \prod_{s\in[1,M]} e_{s,\tau(s)} \;&=\; \sum_{k\in[1,n]} \sum_{s\in I_{(k)}} \deg e_{s,\tau(s)} \;=\; \sum_{k\in[1,n]} \sum_{s\in I_{(k)}} (M_{(k)} - \tau(s) + s - m^{(k-1)}) \\
&=\; \sum_{k\in[1,n]} \sum_{s\in I_{(k)}} (M_{(k)} - m^{(k-1)}) + \sum_{k\in[1,n]} \sum_{s\in I_{(k)}} (-\tau(s) + s) \\
&=\; \sum_{k\in[1,n]} m_{(k)}(M_{(k)} - m^{(k-1)}) \;=\; \sum_{k\in[1,n]} m_{(k)} \sum_{\ell\in[k+1,n]} m_{(\ell)} \;=\; d\,.
\end{aligned}$$

This proves the *claim*. So we have

$$\text{(II)} \qquad \operatorname{Res}(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)}) \;=\; C \,\cdot\, \operatorname{Res}_0(\hat{g}_{(1)}\,,\,\dots\,,\,\hat{g}_{(n)})$$

for some $C \in K$. We want to show that $C = 1$.
Step 3.2. Suppose given $\ell \in [1, n-1]$. Given a monomial $\alpha := c \prod_{k\in[1,n]} \prod_{i\in[1,m_{(k)}]} \hat{\gamma}_{(k)i}^{\,w_{(k)i}}$ in $\hat{L}$, where $w_{(k)i} \in \mathbb{Z}_{\ge 0}$ and $c \in K \smallsetminus \{0\}$, we let $\deg_{(\ell)}(\alpha) := \sum_{i\in[1,m_{(\ell)}]} w_{(\ell)i}$ be the (ℓ)-*degree* of α.

Now we define the degree Deg of a monomial $\beta \in \hat{L}$ to be

$$\operatorname{Deg}(\beta) \;:=\; (\deg_{(1)}(\beta)\,,\,\dots\,,\,\deg_{(n-1)}(\beta)) \;\in\; (\mathbb{Z}_{\ge 0})^{\times(n-1)}$$

and, for $\ell \in [0, n-1]$, the degree $\operatorname{Deg}_{(\ell)}$ of a monomial $\beta \in \hat{L}$ to be

$$\operatorname{Deg}_{(\ell)}(\beta) \;:=\; (\deg_{(1)}(\beta)\,,\,\dots\,,\,\deg_{(\ell)}(\beta)\,,\,0\,,\,\dots\,,\,0) \;\in\; (\mathbb{Z}_{\ge 0})^{\times(n-1)}\,.$$

We define a lexicographical order on $(\mathbb{Z}_{\geq 0})^{\times (n-1)}$ by

$$\begin{aligned} (k_1\,,\,\ldots\,,\,k_{n-1}) \;>\; (k'_1\,,\,\ldots\,,\,k'_{n-1}) \quad :\Leftrightarrow \qquad & (k_1 \;>\; k'_1) \\ \vee \quad & ((k_1 \;=\; k'_1) \,\wedge\, (k_2 \;>\; k'_2)) \\ \vee \quad & ((k_1 \;=\; k'_1) \,\wedge\, (k_2 \;=\; k'_2) \,\wedge\, (k_3 \;>\; k'_3)) \\ \vee \quad & \ldots \\ \vee \quad & ((k_i \;=\; k'_i \text{ for } i \in [1, n-2]) \,\wedge\, (k_{n-1} \;>\; k'_{n-1}))\;. \end{aligned}$$

Abbreviate $\Gamma_{(k)} := \prod_{i\in[1,m_{(k)}]} \hat{\gamma}_{(k)i}$ for $k \in [1,n]$. We want to compare coefficients of the monomial $\Gamma := \prod_{k\in[1,n]} \Gamma_{(k)}^{m^{(k-1)}}$ in $\operatorname{Res}_0(\hat{g}_{(1)},\ldots,\hat{g}_{(n)})$ and $\operatorname{Res}(\hat{g}_{(1)},\ldots,\hat{g}_{(n)})$.
Note that

$$\operatorname{Deg}(\Gamma) \;=\; (\overbrace{m^{(0)}}^{=\,0} m_{(1)}\,,\, m^{(1)}m_{(2)}\,,\,\ldots\,,\, m^{(n-2)}m_{(n-1)})\;. \tag{III}$$

First we consider $\operatorname{Res}_0(\hat{g}_{(1)},\ldots,\hat{g}_{(n)}) \;=\; \prod\limits_{1\leq k<\ell\leq n} \;\prod\limits_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]} (\hat{\gamma}_{(k)i} \;-\; \hat{\gamma}_{(\ell)j})$. Its Deg-minimal monomial, including coefficient, is given by $\prod\limits_{1\leq k<\ell\leq n} \;\prod\limits_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]} (-\,\hat{\gamma}_{(\ell)j})$, for replacing any factor $(-\,\hat{\gamma}_{(\ell)j})$ therein by a factor $\hat{\gamma}_{(k)i}$ with $k < \ell$ strictly raises the degree Deg. We have

$$\begin{aligned} \prod_{1\leq k<\ell\leq n} \;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]} (-\,\hat{\gamma}_{(\ell)j}) \;&=\; (-1)^{\sum\limits_{1\leq k<\ell\leq n} m_{(k)}m_{(\ell)}} \prod_{1\leq k<\ell\leq n} \;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]} \hat{\gamma}_{(\ell)j} \\ =\; (-1)^{\sum\limits_{1\leq k<\ell\leq n} m_{(k)}m_{(\ell)}} \prod_{1\leq k<\ell\leq n} \Gamma_{(\ell)}^{m_{(k)}} \;&=\; (-1)^{\sum\limits_{\ell\in[1,n]}\sum\limits_{k\in[1,\ell-1]} m_{(k)}m_{(\ell)}} \prod_{\ell\in[1,n]}\;\prod_{k\in[1,\ell-1]} \Gamma_{(\ell)}^{m_{(k)}} \\ =\; (-1)^{\sum\limits_{\ell\in[1,n]} m^{(\ell-1)}m_{(\ell)}} \prod_{\ell\in[1,n]} \Gamma_{(\ell)}^{m^{(\ell-1)}} \;&=\; (-1)^{\sum\limits_{\ell\in[1,n]} m^{(\ell-1)}m_{(\ell)}}\, \Gamma\;. \end{aligned}$$

Now consider $\operatorname{Res}(\hat{g}_{(1)},\ldots,\hat{g}_{(n)}) \;=\; \det A(g_{(1)},\ldots,g_{(n)})$; cf. Definition 1. Its diagonal Leibniz-summand, belonging to $\mathrm{id} \in \mathrm{S}_M$, equals $\prod\limits_{k\in[1,n]} \hat{a}_{(k)m^{(k-1)}}^{m_{(k)}}$. Recall that $\sum_{j\in[0,M_{(k)}]} \hat{a}_{(k)j}X^j \;=\; \prod_{\ell\in[1,n]\smallsetminus\{k\}} \hat{g}_{(\ell)}(X) = \prod_{\ell\in[1,n]\smallsetminus\{k\}} \prod_{i\in[1,m_{(\ell)}]} (X - \hat{\gamma}_{(\ell)i})$. So $\hat{a}_{(k)m^{(k-1)}}$ equals the sum of all products of $M_{(k)} - m^{(k-1)} = \sum_{\ell\in[k+1,n]} m_{(\ell)}$ factors of the form $(-\hat{\gamma}_{(\ell)i})$, where $\ell \in [1,n] \smallsetminus \{k\}$ and $i \in [1, m_{(\ell)}]$. Therefore the unique Deg-minimal monomial in $\hat{a}_{(k)m^{(k-1)}}$, including coefficient, is $\prod_{\ell\in[k+1,n]} \prod_{i\in[1,m_{(\ell)}]} (-\,\hat{\gamma}_{(\ell)i})$, for replacing a factor $(-\hat{\gamma}_{(\ell)i})$ therein by a factor $(-\,\hat{\gamma}_{(\ell')i'})$ with $\ell' \in [1, k-1]$ and $i' \in [1, m_{(\ell')}]$ strictly raises the degree Deg. Thus the unique Deg-minimal monomial in $\prod\limits_{k\in[1,n]} \hat{a}_{(k)m^{(k-1)}}^{m_{(k)}}$ equals

$$\begin{aligned} \prod_{k\in[1,n]}\;\prod_{\ell\in[k+1,n]}\;\prod_{i\in[1,m_{(\ell)}]} (-\,\hat{\gamma}_{(\ell)i})^{m_{(k)}} \;&=\; (-1)^{\sum\limits_{k\in[1,n]}\sum\limits_{\ell\in[k+1,n]} m_{(\ell)}m_{(k)}} \prod_{k\in[1,n]}\;\prod_{\ell\in[k+1,n]}\;\prod_{i\in[1,m_{(\ell)}]} \hat{\gamma}_{(\ell)i}^{m_{(k)}} \\ =\; (-1)^{\sum\limits_{k\in[1,n]}\sum\limits_{\ell\in[k+1,n]} m_{(\ell)}m_{(k)}} \prod_{k\in[1,n]}\;\prod_{\ell\in[k+1,n]} \Gamma_{(\ell)}^{m_{(k)}} \;&=\; (-1)^{\sum\limits_{1\leq k<\ell\leq n} m_{(\ell)}m_{(k)}} \prod_{1\leq k<\ell\leq n} \Gamma_{(\ell)}^{m_{(k)}} \\ =\; (-1)^{\sum\limits_{\ell\in[1,n]}\sum\limits_{k\in[1,\ell-1]} m_{(\ell)}m_{(k)}} \prod_{\ell\in[1,n]}\;\prod_{k\in[1,\ell-1]} \Gamma_{(\ell)}^{m_{(k)}} \;&=\; (-1)^{\sum\limits_{\ell\in[1,n]} m_{(\ell)}m^{(\ell-1)}} \prod_{\ell\in[1,n]} \Gamma_{(\ell)}^{m^{(\ell-1)}} \\ =\; (-1)^{\sum\limits_{\ell\in[1,n]} m^{(\ell-1)}m_{(\ell)}}\, \Gamma\;. \end{aligned}$$

So we have to show that the monomial Γ does not appear in another Leibniz-summand.

Recall that $A(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,) \;=\; (e_{s,t})_{s,t} \;\in\; \hat{L}^{M\times M}$.

Suppose given $\tau \;\in\; \mathrm{S}_M$. Suppose that its Leibniz-summand $\prod\limits_{i\in[1,M]} e_{i,\tau(i)}$ in $\det A(\hat{g}_{(1)},\ldots,\hat{g}_{(n)})$ contains a nonzero monomial $\tilde{\Gamma}$ that has degree

$$\text{(IV)}\qquad \mathrm{Deg}(\tilde{\Gamma}) \;\le\; \mathrm{Deg}(\Gamma) \overset{\text{(III)}}{=} (\underbrace{m^{(0)}}_{=0} m_{(1)}\,,\, m^{(1)}m_{(2)}\,,\,\ldots\,,\, m^{(n-2)}m_{(n-1)})\;.$$

It suffices to show that $\tau \overset{!}{=} \mathrm{id}$.

For $k \in [0, n-1]$, we denote by $\tilde{\Gamma}^{(k)}$ the subproduct of $\tilde{\Gamma}$ that consists of those factors of $\tilde{\Gamma}$ that appear as monomials in $e_{i,\tau(i)}$ for $i \in I^{(k)}$. Let $\tilde{\Gamma}^{(-1)} := 1$. So $\tilde{\Gamma}^{(-1)} \;=\; \tilde{\Gamma}^{(0)} \;=\; 1$.

We prove by *induction* on $k \in [0, n-1]$ that

$$1.\ \tau(s) \;=\; s \text{ for } s \in I^{(k)}, \qquad 2.\ \tau(s) \;\ge\; s \text{ for } s \in I_{(k+1)}\,, \qquad 3.\ \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k-1)}) \;=\; \mathrm{Deg}_{(k)}(\Gamma).$$

Putting $k = n-1$ then yields $\tau = \mathrm{id}$. In fact, *assume* that $\tau \ne \mathrm{id}$. Let $s' \in [1, M]$ be minimal such that $\tau(s') \ne s'$. Then $\tau(s') > s'$, and $\tau(s) = s$ for $s \in [1, s'-1]$. So there exists $s'' \in [s'+1, M]$ such that $\tau(s'') = s'$. But $s'' \overset{2.}{\le} \tau(s'') = s' < s''$, ↯.

Base clause for $k \;=\; 0$: We have $I^{(0)} = \emptyset$. We have $\mathrm{Deg}_{(0)}(\tilde{\Gamma}^{(-1)}) \;=\; (0,\ldots,0) \;=\; \mathrm{Deg}_{(0)}(\Gamma)$. We have $\tau(s) \;\ge\; s$ for $s \in I_{(1)}$, since $e_{i,j} = 0$ for $i \in I_{(1)}$ and $j \in [1, i-1]$.

Induction step : Suppose given $k \in [0, n-2]$. By induction assumption, we have

$$1.\ \tau(s) \;=\; s \text{ for } s \in I^{(k)}, \qquad 2.\ \tau(s) \;\ge\; s \text{ for } s \in I_{(k+1)}\,, \qquad 3.\ \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k-1)}) \;=\; \mathrm{Deg}_{(k)}(\Gamma).$$

We have $\mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)}) \le \mathrm{Deg}_{(k)}(\tilde{\Gamma}) \overset{\text{(IV)}}{\le} \mathrm{Deg}_{(k)}(\Gamma) \overset{3.}{=} \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k-1)}) \;\le\; \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)})$, whence

$$\text{(V)}\qquad \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)}) \;=\; \mathrm{Deg}_{(k)}(\tilde{\Gamma}) \;=\; \mathrm{Deg}_{(k)}(\Gamma)\;.$$

We have to show that

$$1!.\ \tau(s) \overset{!}{=} s \text{ for } s \in I^{(k+1)}, \qquad 2!.\ \tau(s) \overset{!}{\ge} s \text{ for } s \in I_{(k+2)}\,, \qquad 3!.\ \mathrm{Deg}_{(k+1)}(\tilde{\Gamma}^{(k)}) \overset{!}{=} \mathrm{Deg}_{(k+1)}(\Gamma).$$

Using (V), it suffices to show that

$$1!.\ \tau(s) \overset{!}{=} s \text{ for } s \in I_{(k+1)}\,, \qquad 2!.\ \tau(s) \overset{!}{\ge} s \text{ for } s \in I_{(k+2)}\,, \qquad 3!.\ \deg_{(k+1)}(\tilde{\Gamma}^{(k)}) \overset{!}{=} \deg_{(k+1)}(\Gamma).$$

We consider 3! first. We *claim* that

$$(-1)^{\sum\limits_{\ell\in[1,k]}(M-m^{(\ell)})m_{(\ell)}} (\Gamma_{(2)}\Gamma_{(3)}\cdots\Gamma_{(n)})^{m_{(1)}} \cdot (\Gamma_{(3)}\cdots\Gamma_{(n)})^{m_{(2)}} \cdot \ldots \cdot (\Gamma_{(k+1)}\cdots\Gamma_{(n)})^{m_{(k)}} \overset{!}{=} \tilde{\Gamma}^{(k)}\;.$$

We prove by *induction* on $\ell \in [1, k]$ that for $i \in I_{(\ell)}$, the monomial of $e_{i,\tau(i)} \overset{1.}{=} e_{i,i} \;=\; \hat{a}_{(\ell)m^{(\ell-1)}}$ that appears as a factor in $\tilde{\Gamma}$ equals $(-1)^{M-m^{(\ell)}}\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}$. Since $|I_{(\ell)}| = m_{(\ell)}$ for $\ell \in [1, k]$, this then will prove the claim.

Base clause $\ell \;=\; 1$: Since $\hat{a}_{(1),m^{(0)}}$ is the constant coefficient of $\prod\limits_{\kappa\in[2,n]} \hat{g}_{(\kappa)}(X) \;=\; \prod\limits_{\kappa\in[2,n]}\; \prod\limits_{j\in[1,m_{(\kappa)}]} (X - \hat{\gamma}_{(\kappa)j})$, it consists of only one summand, namely $(-1)^{M-m^{(1)}}\Gamma_{(2)}\cdots\Gamma_{(n)}$.

Induction step : Suppose given $\ell \in [1, k-1]$. Since, by induction assumption, $(-1)^{M-m^{(\lambda)}}\Gamma_{(\lambda+1)}\cdots\Gamma_{(n)}$ is the monomial of $\hat{a}_{(\lambda)m^{(\lambda-1)}}$ that appears as a factor in $\tilde{\Gamma}$ with multiplicity $m_{(\lambda)}$ for $\lambda \in [1, \ell-1]$, we have

$$\begin{aligned}
\tilde{\Gamma}^{(\ell-1)} &= \prod_{\lambda\in[1,\ell-1]} \big((-1)^{M-m^{(\lambda)}}\Gamma_{(\lambda+1)}\cdots\Gamma_{(n)}\big)^{m_{(\lambda)}} \\
&= (-1)^{\sum\limits_{\lambda\in[1,\ell-1]}(M-m^{(\lambda)})m_{(\lambda)}} \big(\prod_{\lambda\in[1,\ell-1]} \big(\Gamma_{(\lambda+1)}\cdots\Gamma_{(\ell)}\big)^{m_{(\lambda)}}\big)\cdot\big(\prod_{\lambda\in[1,\ell-1]} \big(\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}\big)^{m_{(\lambda)}}\big) \\
&= (-1)^{\sum\limits_{\lambda\in[1,\ell-1]}(M-m^{(\lambda)})m_{(\lambda)}} \big(\Gamma_{(1)}^{m^{(0)}}\Gamma_{(2)}^{m^{(1)}}\cdots\Gamma_{(\ell)}^{m^{(\ell-1)}}\big)\cdot\big(\prod_{\lambda\in[1,\ell-1]} \big(\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}\big)^{m_{(\lambda)}}\big),
\end{aligned}$$

whence $\deg_{(\lambda)}(\tilde{\Gamma}^{(\ell-1)}) = \deg_{(\lambda)}(\Gamma_{(\lambda)}^{m^{(\lambda-1)}}) = m^{(\lambda-1)}m_{(\lambda)} = \deg_{(\lambda)}(\Gamma)$ for $\lambda \in [1, \ell-1]$.

Suppose given $i \in I_{(\ell)}$. Let φ be the monomial of $e_{i,\tau(i)} = e_{i,i} = \hat{a}_{(\ell)m^{(\ell-1)}}$ that appears as a factor in $\tilde{\Gamma}$. We have to show that $\varphi \overset{!}{=} (-1)^{M-m^{(\ell)}}\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}$.

Suppose given $\lambda \in [1, \ell-1]$. Since $\mathrm{Deg}_{(k)}(\tilde{\Gamma}) = \mathrm{Deg}_{(k)}(\Gamma)$ by (V), we in particular have $\deg_{(\lambda)}(\tilde{\Gamma}) = \deg_{(\lambda)}(\Gamma)$. Since $\deg_{(\lambda)}(\tilde{\Gamma}^{(\ell-1)}) = \deg_{(\lambda)}(\Gamma)$ by the consideration above, the monomial φ is not divisible by $\hat{\gamma}_{(\lambda)j}$ for $j \in [1, m_{(\lambda)}]$. Recall that $\hat{a}_{(\ell)m^{(\ell-1)}}$ is the coefficient of $X^{m^{(\ell-1)}}$ of the polynomial $\prod\limits_{\kappa\in[1,n]\smallsetminus\{\ell\}} \hat{g}_{(\kappa)}(X) = \prod\limits_{\kappa\in[1,n]\smallsetminus\{\ell\}}\ \prod\limits_{j\in[1,m_{(\kappa)}]} (X - \hat{\gamma}_{(\kappa)j})$. Expanding this polynomial, the terms contributing to φ may not contain a factor $(-\hat{\gamma}_{(\kappa)j})$ with $\kappa \in [1, \ell-1]$. Thus the only term that contributes to φ is

$$\big(\prod_{\kappa\in[1,\ell-1]}\ \prod_{j\in[1,m_{(\kappa)}]} X\big)\cdot\big(\prod_{\kappa\in[\ell+1,n]}\ \prod_{j\in[1,m_{(\kappa)}]} (-\hat{\gamma}_{(\kappa)j})\big) = X^{m^{(\ell-1)}}\cdot(-1)^{M-m^{(\ell)}}\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}\,,$$

whence the result for φ. This concludes the *induction* thus proves this *claim*.

Taking $(k+1)$-degrees, this claim yields

$$\begin{aligned}
\deg_{(k+1)}(\tilde{\Gamma}^{(k)}) &= \deg_{(k+1)}\big((\Gamma_{(2)}\Gamma_{(3)}\cdots\Gamma_{(n)})^{m_{(1)}}\cdot(\Gamma_{(3)}\cdots\Gamma_{(n)})^{m_{(2)}}\cdot\ldots\cdot(\Gamma_{(k+1)}\cdots\Gamma_{(n)})^{m_{(k)}}\big) \\
&= \deg_{(k+1)}(\Gamma_{(k+1)}^{m_{(1)}+\cdots+m_{(k)}}) = m^{(k)}m_{(k+1)} \overset{\text{(III)}}{=} \deg_{(k+1)}(\Gamma)\,.
\end{aligned}$$

So assertion 3! is shown.

We prove 2! in a stronger form, which will be needed for the proof of 1! later on.

Suppose given $x \in [1, n-k-1]$. Suppose given $s \in I_{(k+1+x)}$. Let φ be the monomial of $e_{s,\tau(s)}$ that appears as a factor in $\tilde{\Gamma}$. Since $\mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)}) \overset{\text{(V)}}{=} \mathrm{Deg}_{(k)}(\tilde{\Gamma})$, we have $\deg_{(\ell)}(\varphi) = 0$ for $\ell \in [1, k]$. Since $\deg_{(k+1)}(\Gamma) \overset{\text{(IV),(V)}}{\geq} \deg_{(k+1)}(\tilde{\Gamma}) \geq \deg_{(k+1)}(\tilde{\Gamma}^{(k)}) \overset{3!}{=} \deg_{(k+1)}(\Gamma)$, we have $\deg_{(k+1)}(\tilde{\Gamma}) = \deg_{(k+1)}(\tilde{\Gamma}^{(k)})$. Thus $\deg_{(k+1)}(\varphi) = 0$. Altogether, $\deg_{(\ell)}(\varphi) = 0$ for $\ell \in [1, k+1]$.

Note that $e_{s,\tau(s)} = \hat{a}_{(k+1+x)\ \tau(s)-s+m^{(k+x)}}$ is the coefficient of $X^{\tau(s)-s+m^{(k+x)}}$ in the polynomial $\prod\limits_{\kappa\in[1,n]\smallsetminus\{k+1+x\}} \hat{g}_{(\kappa)}(X) = \prod\limits_{\kappa\in[1,n]\smallsetminus\{k+1+x\}}\ \prod\limits_{j\in[1,m_{(\kappa)}]} (X - \hat{\gamma}_{(\kappa)j})$. Expanding, we see that φ is a monomial of a coefficient of $\big(\prod\limits_{\kappa\in[1,k+1]}\ \prod\limits_{j\in[1,m_{(\kappa)}]} X\big)\cdot\big(\prod\limits_{\kappa\in[k+2,n]\smallsetminus\{k+1+x\}}\ \prod\limits_{j\in[1,m_{(\kappa)}]} (X - \hat{\gamma}_{(\kappa)j})\big)$. In particular, $\tau(s) - s + m^{(k+x)} \geq m^{(k+1)}$. This is equivalent to

$$\text{(VI)} \qquad \tau(s) \geq s - m^{(k+x)} + m^{(k+1)}.$$

For $x = 1$, assertion 2! is shown.

Now we do 1! by proof of contradiction. *Assume* that $\tau(s_1) \neq s_1$ for some $s_1 \in I_{(k+1)}$. There exists $s_0 \in I_{(k+1)}$ such that $\tau(s) = s$ for $s \in [1, s_0 - 1]$ and $\tau(s_0) > s_0$; cf. 2. Let $\tilde{s} := \tau^{-1}(s_0)$. Then $\tau(\tilde{s}) = s_0$. We have $\tilde{s} \in [s_0 + 1, M]$; cf. 1. If $\tilde{s} \in [s_0 + 1, m^{(k+1)}] \subseteq I_{(k+1)}$, then $s_0 = \tau(\tilde{s}) \overset{2.}{\geq} \tilde{s} \geq s_0 + 1$, $\lightning$. If $\tilde{s} \in I_{(k+1+x)}$ for some $x \in [1, n-k-1]$, then

$$m^{(k+1)} \geq s_0 = \tau(\tilde{s}) \overset{\text{(VI)}}{\geq} \tilde{s} - m^{(k+x)} + m^{(k+1)} \geq (m^{(k+x)} + 1) - m^{(k+x)} + m^{(k+1)} = m^{(k+1)} + 1, \ \lightning\ .$$

So $\tau(s) = s$ for $s \in I_{(k+1)}$ and 1! is shown. This concludes the *induction.*

Step 3.3. To obtain the statement of the lemma, we apply the K-algebra homomorphism

$$\hat{L} \xrightarrow{\rho} L\,, \quad \hat{\gamma}_{(x)\kappa} \longmapsto \gamma_{(x)\kappa} \quad \text{for } x \in [1,n] \text{ and } \kappa \in [1, m_{(x)}]$$

to the preceding equation. So

$$\begin{array}{rclcl} \operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) & = & \rho(\operatorname{Res}(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)})) & = & \rho(\operatorname{Res}_0(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)})) \\ & = & \operatorname{Res}_0(g_{(1)}, \ldots, g_{(n)}) & = & \prod\limits_{1 \leq k < \ell \leq n} \ \prod\limits_{(i,j) \in [1,m_{(k)}] \times [1,m_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j}). \end{array}$$

□

Corollary 3. *We have* $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) = \prod\limits_{1 \leq k < \ell \leq n} \operatorname{Res}(g_{(k)}, g_{(\ell)})$.

Corollary 4. *We have* $\Delta(g_{(1)} \cdot \ldots \cdot g_{(n)}) = \big(\prod\limits_{k \in [1,n]} \Delta(g_{(k)})\big) \cdot \operatorname{Res}(g_{(1)}, \ldots, g_{(n)})^2$.

Proof. Note that $\Delta(g_{(k)}) = \prod\limits_{1 \leq i < j \leq m_{(k)}} (\gamma_{(k)i} - \gamma_{(k)j})^2$ for $k \in [1,n]$; cf. [**6,** §33]. So

$$\begin{array}{l} \Delta(g_{(1)} \cdot \ldots \cdot g_{(n)}) \\ \quad = \ \Big(\prod\limits_{k \in [1,n]} \prod\limits_{1 \leq i < j \leq m_{(k)}} (\gamma_{(k)i} - \gamma_{(k)j})^2\Big) \cdot \Big(\prod\limits_{1 \leq k < \ell \leq n} \ \prod\limits_{(i,j) \in [1,m_{(k)}] \times [1,m_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j})^2\Big) \\ \quad \overset{\text{Lem. 2}}{=} \ \Big(\prod\limits_{k \in [1,n]} \Delta(g_{(k)})\Big) \cdot \operatorname{Res}(g_{(1)}, \ldots, g_{(n)})^2 . \end{array}$$

□

Remark 5. *Let* $r \in R$. *Let* $f(X), \tilde{f}(X) \in R[X]$ *monic polynomials such that* $f(X) \equiv_r \tilde{f}(X)$. *Then* $\Delta(f) \equiv_r \Delta(\tilde{f})$.

Remark 6. *Let* $f(X) \in R[X]$ *be a monic polynomial with* $\Delta(f) \neq 0$. *Suppose that we have* $f(X) \equiv_{\pi\Delta(f)} \prod\limits_{k \in [1,n]} g_{(k)}(X)$. *Then* $2\, \mathrm{v}_\pi(\operatorname{Res}(g_{(1)}, \ldots, g_{(n)})) \leq \mathrm{v}_\pi(\Delta(f))$.

Proof. We have $\Delta(f) \overset{\text{R 5}}{\equiv}_{\pi\Delta(f)} \Delta(\prod\limits_{k \in [1,n]} g_{(k)}) \overset{\text{C 4}}{=} \big(\prod\limits_{k \in [1,n]} \Delta(g_{(k)})\big) \cdot \operatorname{Res}(g_{(1)}, \ldots, g_{(n)})^2$. □

Remark 7. *Let* $r \in R$. *Let* $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ *be monic polynomials such that* $g_{(k)}(X) \equiv_r \tilde{g}_{(k)}(X)$ *for* $k \in [1,n]$. *Then* $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) \equiv_r \operatorname{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})$.

Proof. Note that $\deg g_{(k)} = \deg \tilde{g}_{(k)}$ for $k \in [1,n]$. Hence $A(g_{(1)}, \ldots, g_{(n)}) \equiv_r A(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})$; cf. Definition 1. Taking determinants, we get $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) \equiv_r \operatorname{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})$. □

2 Hensel

Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

2.1 Linear Algebra

Suppose given $k \geq 1$. Suppose given $A \in R^{k\times k}$ such that $\det(A) \neq 0$. Let $\pi^{e_1}, \ldots, \pi^{e_k}$ be the elementary divisors of A, ordered such that $0 \leq e_1 \leq e_2 \leq \cdots \leq e_k$. Write $e := e_1 + \cdots + e_k = \mathrm{v}_\pi(\det(A))$. Choose $S, T \in \mathrm{GL}_k(R)$ such that $SAT = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_k}) =: D$. Suppose given $d_i \in \mathbb{Z}_{\geq 0}$ for $i \in [1,k]$ such that $d_1 \geq d_2 \geq \cdots \geq d_k$. Write $e' := e - (d_2 + \cdots + d_k)$.

Remark 8. *Suppose that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A. Then $0 \leq e_k \leq e'$.*

Proof. Each $(k-1)\times(k-1)$-minor of A is divisible by $\pi^{d_k+\cdots+d_2}$. So $\pi^{d_k+\cdots+d_2}$ divides their greatest common divisor π^{e-e_k}. □

Lemma 9.

(1) *Suppose given $y \in \pi^{e_k}R^{1\times k}$. Then there exists $x \in R^{1\times k}$ such that $xA = y$.*

(2) *Suppose given $y \in \pi^{e}R^{1\times k}$. Then there exists $x \in R^{1\times k}$ such that $xA = y$.*

(3) *Suppose that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A. Suppose given $y \in \pi^{e'}R^{1\times k}$. Then there exists $x \in R^{1\times k}$ such that $xA = y$.*

Proof. Ad (1). Write $yT = (\pi^{e_k}z_1, \ldots, \pi^{e_k}z_k)$, where $z_i \in R$ for $i \in [1,k]$. Let $x := (\pi^{e_k-e_1}z_1, \ldots, \pi^{e_k-e_k}z_k)S \in R^{1\times k}$. So $xA = xS^{-1}DT^{-1} = (\pi^{e_k-e_1}z_1, \ldots, \pi^{e_k-e_k}z_k)DT^{-1} = yTT^{-1} = y$.

Ad (3). By Remark 8 we have $e' \geq e_k$, so that the assertion follows with (1). □

Lemma 10.

(1) *Suppose given $u \geq e_k$ and $x \in R^{1\times k}$ such that $xA \in R^{1\times k}\pi^u$. Then $x \in R^{1\times k}\pi^{u-e_k}$.*

(2) *Suppose given $u \geq e$ and $x \in R^{1\times k}$ such that $xA \in R^{1\times k}\pi^u$. Then $x \in R^{1\times k}\pi^{u-e}$.*

(3) *Suppose that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A. Suppose given $u \geq e'$ and $x \in R^{1\times k}$ such that $xA \in R^{1\times k}\pi^u$. Then $x \in R^{1\times k}\pi^{u-e'}$.*

Proof. Ad (1). We have $xA = xS^{-1}DT^{-1} \in R^{1\times k}\pi^u$, whence $xS^{-1}D \in R^{1\times k}\pi^u$. Denote $xS^{-1} =: (z_1, \ldots, z_k) \in R^{1\times k}$. So $xS^{-1}D = (\pi^{e_1}z_1, \ldots, \pi^{e_k}z_k)$. Hence $z_i \in R\pi^{u-e_i} \subseteq R\pi^{u-e_k}$ for $i \in [1,k]$. So $xS^{-1} = (z_1, \ldots, z_k) \in R^{1\times k}\pi^{u-e_k}$. Hence $x \in R^{1\times k}\pi^{u-e_k}S = R^{1\times k}\pi^{u-e_k}$.

Ad (3). By Remark 8 we have $e' \geq e_k$, so that the assertion follows with (1). □

2.2 General case

Let $f(X) \in R[X]$ be a monic polynomial. Write $M := \deg f$.

Let $n \geq 1$. Let $g_{(1)}(X)\,,\ \dots\,,\ g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1 such that $\operatorname{Res}(g_{(1)}\,,\ \dots\,,\ g_{(n)}) \neq 0$. Denote $t := \mathrm{v}_\pi(\operatorname{Res}(g_{(1)}\,,\ \dots\,,\ g_{(n)}))$. Write $m_{(k)} := \deg g_{(k)}$ and $M_{(k)} := M - m_{(k)}$ for $k \in [1,n]$.

Let $s \geq 2t+1$. Suppose that $f(X) \equiv_{\pi^s} \prod\limits_{k\in[1,n]} g_{(k)}(X)\,.$

(Note that we may replace $s \geq 2t+1$ by $s \geq \mathrm{v}_\pi(\Delta(f)) + 1$ if $\Delta(f) \neq 0$; cf. Remark 6.)

Lemma 11 (cf. [**4,** p. 81])**.**

(1) *There exist monic polynomials $\tilde{g}_{(1)}(X)\,,\ \dots\,,\ \tilde{g}_{(n)}(X) \in R[X]$ such that $\tilde{g}_{(k)}(X) \ \equiv_{\pi^{s-t}}\ g_{(k)}(X)$ for $k \in [1,n]$ and $f(X) \ \equiv_{\pi^{2(s-t)}}\ \prod\limits_{k\in[1,n]} \tilde{g}_{(k)}(X)\,.$*

We call such a tuple $(\tilde{g}_{(k)}(X))_k$ of polynomials an admissible lift *of $(g_{(k)}(X))_k$ with respect to s. We have $\mathrm{v}_\pi(\operatorname{Res}(\tilde{g}_{(1)}\,,\ \dots\,,\ \tilde{g}_{(n)})) \ = \ t$ for any admissible lift $(\tilde{g}_{(k)}(X))_k$ of $(g_{(k)}(X))_k$ with respect to s.*

(2) *Suppose given $r \in [0, s-2t]$. Suppose given monic polynomials $\tilde{g}_{(1)}(X)\,,\ \dots\,,\ \tilde{g}_{(n)}(X)$, $\tilde{h}_{(1)}(X)\,,\ \dots\,,\ \tilde{h}_{(n)}(X) \in R[X]$ such that $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ and $\tilde{h}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$, and $\prod\limits_{k\in[1,n]} \tilde{g}_{(k)}(X) \equiv_{\pi^{2(s-t)-r}} \prod\limits_{k\in[1,n]} \tilde{h}_{(k)}(X)$. Then $\tilde{g}_{(k)}(X) \ \equiv_{\pi^{2s-3t-r}}\ \tilde{h}_{(k)}(X)$ for $k \in [1,n]$. In particular, considering the case $r = 0$, two admissible lifts with respect to s as in (1) are mutually congruent modulo $\pi^{2s-3t}R[X]$.*

In the following proof, we shall use the notation of § 1. The arguments we have learnt from Koch, [**5,** Satz 4.4.3, Hilfssatz 4.4.4, Hilfssatz 4.4.5].

Proof. Ad (1). *Existence of admissible lift.*

We make the ansatz $\tilde{g}_{(k)}(X) \ = \ g_{(k)}(X) + \pi^{s-t} u_{(k)}(X)$ for $k \in [1,n]$ with $u_{(k)}(X) \in R[X]$ and $\deg u_{(k)} < \deg g_{(k)} = m_{(k)}$ for $k \in [1,n]$. Thus we require that

$$
\begin{aligned}
f(X) \ \overset{!}{\equiv}_{\pi^{2(s-t)}}\ & \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \ = \ \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t} u_{(k)}(X)) \\
\equiv_{\pi^{2(s-t)}}\ & \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,.
\end{aligned}
$$

Let $b(X) := \pi^{t-s}(f(X) - \prod\limits_{k\in[1,n]} g_{(k)}(X))$. Since $f(X) \equiv_{\pi^s} \prod\limits_{k\in[1,n]} g_{(k)}(X)$, we get $b(X) \equiv_{\pi^t} 0$. So our requirement reads $b(X) \ \overset{!}{\equiv}_{\pi^{s-t}} \sum\limits_{k\in[1,n]} u_{(k)}(X) \cdot \prod\limits_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$. So it suffices to find $u_{(k)}(X) \in R[X]$ for $k \in [1,n]$ as above such that $b(X) \overset{!}{=} \sum\limits_{k\in[1,n]} u_{(k)}(X) \cdot \prod\limits_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,.$

Writing $b(X) =: \sum\limits_{i\geq 0} \beta_i X^i\,,$ $\prod\limits_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) =: \sum\limits_{i\geq 0} a_{(k)i} X^i\,,$ $u_{(k)}(X) =: \sum\limits_{i\geq 0} u_{(k)i} X^i$ for $k \in [1,n]$, where $\beta_i\,,\ a_{(k)i}\,,\ u_{(k)i} \in R$ for $i \geq 0$, a comparison of coefficients shows that it suffices to find

$$
U \ := \ (\underbrace{u_{(1)\,0}\ \dots\ u_{(1)\,m_{(1)}-1}}\ \underbrace{u_{(2)\,0}\ \dots\ u_{(2)\,m_{(2)}-1}}\ \ \dots\ \ \underbrace{u_{(n)\,0}\ \dots\ u_{(n)\,m_{(n)}-1}}) \ \in \ R^{1\times M}
$$

such that

$$U \cdot \underbrace{\left(\begin{array}{ccccccc|l} a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & & & \\ & \ddots & & & & \ddots & & \Big\} \ m_{(1)} \text{ rows} \\ & & a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & \\ a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & & & \\ & \ddots & & & & \ddots & & \Big\} \ m_{(2)} \text{ rows} \\ & & a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & \\ \vdots & & \vdots & & \vdots & & \vdots & \\ \vdots & & \vdots & & \vdots & & \vdots & \\ a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & & & \\ & \ddots & & & & \ddots & & \Big\} \ m_{(n)} \text{ rows} \\ & & a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & \end{array}\right)}_{= \ A(g_{(1)}\,,\ \ldots\ ,\ g_{(n)})} \ \overset{!}{=} \ (\beta_0 \ \ldots \ \beta_{M-1}).$$

Note that $(\beta_0 \ \ldots \ \beta_{M-1}) \in \pi^t R^{1\times M}$ since $b(X) \equiv_{\pi^t} 0$. So U exists as required by Lemma 9.(2).

Valuation of resultant. Since $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$, Remark 7 implies that $\operatorname{Res}(\tilde{g}_{(1)}\,, \ldots, \tilde{g}_{(n)}) \equiv_{\pi^{s-t}} \operatorname{Res}(g_{(1)}\,, \ldots, g_{(n)})$. Since $s-t \geq t+1 = \mathrm{v}_\pi(\operatorname{Res}(g_{(1)}\,, \ldots, g_{(n)}))+1$, this implies $\mathrm{v}_\pi(\operatorname{Res}(\tilde{g}_{(1)}\,, \ldots, \tilde{g}_{(n)})) = \mathrm{v}_\pi(\operatorname{Res}(g_{(1)}\,, \ldots, g_{(n)})) = t$.

Ad (2). Writing $\tilde{g}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t}u_{(k)}(X)$ and $\tilde{h}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t}v_{(k)}(X)$ for $k \in [1,n]$, where $u_{(k)}(X), v_{(k)}(X) \in R[X]$, we obtain $\deg u_{(k)}(X) < \deg g_{(k)}(X) = m_{(k)}$, since $\tilde{g}_{(k)}(X)$ and $g_{(k)}(X)$ are monic polynomials of the same degree; likewise, we obtain $\deg v_{(k)}(X) < m_{(k)}$.

We have to show that $u_{(k)}(X) \overset{!}{\equiv}_{\pi^{s-2t-r}} v_{(k)}(X)$ for $k \in [1,n]$. We have

$$\begin{aligned} \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ &\equiv_{\pi^{2(s-t)}} \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t}u_{(k)}(X)) \\ &= \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \ \equiv_{\pi^{2(s-t)-r}} \prod_{k\in[1,n]} \tilde{h}_{(k)}(X) \\ = \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t}v_{(k)}(X)) \ &\equiv_{\pi^{2(s-t)}} \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t} \sum_{k\in[1,n]} v_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,. \end{aligned}$$

The difference yields $\sum_{k\in[1,n]} (u_{(k)}(X) - v_{(k)}(X)) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \equiv_{\pi^{s-t-r}} 0\,.$

Writing $w_{(k)}(X) := u_{(k)}(X) - v_{(k)}(X)$ for $k \in [1,n]$, this reads

$$(*) \qquad \sum_{k\in[1,n]} w_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ \equiv_{\pi^{s-t-r}} \ 0\,.$$

Writing $w_{(k)}(X) =: \sum_{i\geq 0} w_{(k)i}X^i$ for $k \in [1,n]$, and

$$W := (\underbrace{w_{(1)\,0} \ \ldots \ w_{(1)\,m_{(1)}-1}} \ \underbrace{w_{(2)\,0} \ \ldots \ w_{(2)\,m_{(2)}-1}} \ \ \cdots \ \ \underbrace{w_{(n)\,0} \ \ldots \ w_{(n)\,m_{(n)}-1}}) \in R^{1\times M}\,,$$

we have to show that $W \overset{!}{\in} \pi^{s-2t-r}R^{1\times M}$. From $(*)$, we obtain $W \cdot A(g_{(1)}\,, \ldots, g_{(n)}) \in \pi^{s-t-r}R^{1\times M}$. Note that $s-t-r \geq t = \mathrm{v}_\pi(\det A(g_{(1)}\,, \ldots, g_{(n)}))$. So we can infer by Lemma 10.(2) that $W \in \pi^{s-2t-r}R^{1\times M}$. □

Theorem 12. *Suppose R to be complete.*
Then there exist unique monic polynomials $\overset{\vee}{g}_{(1)}(X)\,,\;\dots\;,\;\overset{\vee}{g}_{(n)}(X) \in R[X]$ such that $\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$ and $f(X) = \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)$.

Proof. Existence. Since R is complete, it suffices to show that there exist monic polynomials $\tilde{g}_{(1)}(X)\,,\;\dots\;,\;\tilde{g}_{(n)}(X) \in R[X]$ such that $f(X) \equiv_{\pi^{s+1}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X)$ and $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$, and $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}\,,\;\dots\;,\;\tilde{g}_{(n)})) = t$. This follows by Lemma 11.(1) as $2(s-t) \geq s+1$.

Uniqueness. Given $\overset{\vee}{g}_{(1)}(X), \dots, \overset{\vee}{g}_{(n)}(X), \overset{\vee}{h}_{(1)}(X), \dots, \overset{\vee}{h}_{(n)}(X) \in R[X]$, all monic, such that $\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X) \equiv_{\pi^{s-t}} \overset{\vee}{h}_{(k)}(X)$ for $k \in [1,n]$ and $\prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) = f(X) = \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X)$, we have to show that $\overset{\vee}{g}_{(k)}(X) \overset{!}{=} \overset{\vee}{h}_{(k)}(X)$ for $k \in [1,n]$.

Note that $\mathrm{v}_\pi(\mathrm{Res}(\overset{\vee}{g}_{(1)}\,,\;\dots\;,\;\overset{\vee}{g}_{(n)})) = t = \mathrm{v}_\pi(\mathrm{Res}(\overset{\vee}{h}_{(1)}\,,\;\dots\;,\;\overset{\vee}{h}_{(n)}))$ by Lemma 11.(1).

Let $s_1 := s$. Both $(\overset{\vee}{h}_{(k)}(X))_k$ and $(\overset{\vee}{g}_{(k)}(X))_k$ are admissible lifts of $(\overset{\vee}{g}_{(k)}(X))_k$ with respect to s_1 in the sense of Lemma 11.(1), since $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_1-t}} \overset{\vee}{g}_{(k)}(X)$ for $k \in [1,n]$ and the other required congruences are verified using equalities. So Lemma 11.(2) yields $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_1-t)-t}} \overset{\vee}{g}_{(k)}(X)$ for $k \in [1,n]$.

Let $s_2 := 2(s_1 - t)$. Note that $s_2 = s_1 + (s_1 - 2t) > s_1$. Both $(\overset{\vee}{h}_{(k)}(X))_k$ and $(\overset{\vee}{g}_{(k)}(X))_k$ are admissible lifts of $(\overset{\vee}{g}_{(k)}(X))_k$ with respect to s_2, since $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_2-t}} \overset{\vee}{g}_{(k)}(X)$ for $k \in [1,n]$. So Lemma 11.(2) yields $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_2-t)-t}} \overset{\vee}{g}_{(k)}(X)$ for $k \in [1,n]$.

Let $s_3 := 2(s_2 - t)$. Note that $s_3 = s_2 + (s_2 - 2t) > s_2 + (s_1 - 2t) > s_2$. Continue as above.

This yields a strictly increasing sequence $(s_\ell)_{\ell\geq 1}$ of integers such that $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_\ell-t}} \overset{\vee}{g}_{(k)}(X)$ for $k \in [1,n]$ and $\ell \geq 1$. Hence $\overset{\vee}{h}_{(k)}(X) = \overset{\vee}{g}_{(k)}(X)$ for $k \in [1,n]$. □

Remark 13. The case $n = 2$ of Theorem 12, i.e. the case of a factorisation of $f(X)$ into two factors $g_{(1)}(X)$ and $g_{(2)}(X)$ modulo π^s, is due to Hensel; cf. [**4,** p. 80, 81].

Translated to our notation, he starts right away with $s > t$. He writes in the statement on [**4,** p. 80, l. 8] that $\overset{\vee}{g}_{(1)}(X)$ and $\overset{\vee}{g}_{(2)}(X)$ are "Näherungswerte" of $g_{(1)}(X)$ and $g_{(2)}(X)$. In the proof, on [**4,** p. 81, l. 7], he makes this precise and shows that actually $\overset{\vee}{g}_{(1)}(X) \equiv_{\pi^{s-t}} g_{(1)}(X)$ and $\overset{\vee}{g}_{(2)}(X) \equiv_{\pi^{s-t}} g_{(2)}(X)$.

Example 14. Suppose that $n = 3$. Write $t_0 := \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\; g_{(3)}))$, $t_1 := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\; g_{(2)}g_{(3)}))$. Lemma 2 gives $\mathrm{Res}(g_{(1)}\,,\; g_{(2)}\,,\; g_{(3)}) = \mathrm{Res}(g_{(1)}\,,\; g_{(2)}g_{(3)}) \cdot \mathrm{Res}(g_{(2)}\,,\; g_{(3)})$, whence $t = t_1 + t_0$. In particular, $\mathrm{Res}(g_{(1)}\,,\; g_{(2)}g_{(3)}) \neq 0$ and $\mathrm{Res}(g_{(2)}\,,\; g_{(3)}) \neq 0$.

We can apply Lemma 11.(1) to $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ to obtain monic polynomials $\tilde{g}_{(1)}(X)\,,\; \tilde{g}_{(2)}(X)\,,\; \tilde{g}_{(3)}(X) \in R[X]$ such that

(i) $\quad \tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,3]\,,\quad f(X) \equiv_{\pi^{2(s-t)}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) \cdot \tilde{g}_{(3)}(X)\,.$

We can also apply Lemma 11.(1) first to the factorisation $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot (g_{(2)}(X) \cdot g_{(3)}(X))$ and then to the resulting factorisation of the second factor into $g_{(2)}(X) \cdot g_{(3)}(X)$ modulo a certain power of π.

We have $s \geq 2t{+}1 \geq 2t_1{+}1$. So Lemma 11.(1) gives monic polynomials $\tilde{h}_{(1)}(X)$, $\tilde{h}_{(2)}(X) \in R[X]$ such that

$$\tilde{h}_{(1)}(X) \equiv_{\pi^{s-t_1}} g_{(1)}(X)\,, \quad \tilde{h}_{(2)}(X) \equiv_{\pi^{s-t_1}} g_{(2)}(X) \cdot g_{(3)}(X)\,, \quad f(X) \equiv_{\pi^{2(s-t_1)}} \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X)\,.$$

We have $s - t_1 \geq 2t + 1 - t_1 = t_1 + 2t_0 + 1 \geq 2t_0 + 1$. So Lemma 11.(1) gives monic polynomials $\tilde{\tilde{g}}_{(2)}(X)$, $\tilde{\tilde{g}}_{(3)}(X) \in R[X]$ such that

$$\begin{aligned} \tilde{\tilde{g}}_{(2)}(X) \equiv_{\pi^{(s-t_1)-t_0}} g_{(2)}(X)\,, \quad \tilde{\tilde{g}}_{(3)}(X) \equiv_{\pi^{(s-t_1)-t_0}} g_{(3)}(X)\,, \\ \tilde{h}_{(2)}(X) \equiv_{\pi^{2((s-t_1)-t_0)}} \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X)\,. \end{aligned}$$

Altogether, the two subsequent applications of Lemma 11.(1) for two factors yield

$$\text{(ii)} \qquad \begin{array}{l} \tilde{h}_{(1)}(X) \equiv_{\pi^{s-t_1}} g_{(1)}(X)\,.\ \tilde{\tilde{g}}_{(2)}(X) \equiv_{\pi^{s-t_1-t_0}} g_{(2)}(X)\,, \ \tilde{\tilde{g}}_{(3)}(X) \equiv_{\pi^{s-t_1-t_0}} g_{(3)}(X) \\ f(X) \equiv_{\pi^{2(s-t_1)}} \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \equiv_{\pi^{2(s-t_1-t_0)}} \tilde{h}_{(1)}(X) \cdot \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X)\,. \end{array}$$

Comparing the result (i) of Lemma 11.(1) for three factors with the result (ii) of two subsequent applications of Lemma 11.(1) for two factors, both methods essentially yield a precision of $s - t$ for the factors and a precision of $2(s - t)$ for the product decomposition.

2.3 Case $f(X) \equiv_\pi X^M$

Let $f(X) \in R[X]$ be a monic polynomial. Write $M := \deg f$. Suppose that $f(X) \equiv_\pi X^M$.

Let $n \geq 1$. Suppose given monic polynomials $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ with degree ≥ 1. Write $m_{(k)} := \deg(g_{(k)})$ and $M_{(k)} := M - m_{(k)}$ for $k \in [1, n]$. Suppose the ordering to be chosen such that $m_{(1)} \leq m_{(2)} \leq \cdots \leq m_{(n)}$ and that $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) \neq 0$. Let $t := \mathrm{v}_\pi\big(\operatorname{Res}(g_{(1)}, \ldots, g_{(n)})\big)$, $t' := e' := \mathrm{v}_\pi\big(\operatorname{Res}(g_{(1)}\,, \ldots\,, g_{(n)})\big) - \sum_{j \in [1,n-1]} \big((n-j)m_{(j)} - 1\big)$. Let $s \geq t + t' + 1$. Suppose that $f(X) \equiv_{\pi^s} \prod\limits_{k \in [1,n]} g_{(k)}(X)$. We remark that $g_{(k)}(X) \equiv_\pi X^{m_{(k)}}$ for $k \in [1, n]$.

(Note that we may replace $s \geq t + t' + 1$ by $s \geq \mathrm{v}_\pi(\Delta(f)) + 1$ if $\Delta(f) \neq 0$; cf. Remark 6.)

Lemma 15. *Let $\ell \geq 1$. Let $h_{(1)}(X)\,, \ldots\,, h_{(\ell)}(X) \in R[X]$ be monic polynomials of degree ≥ 1. Write $\chi_{(k)} := \deg(h_{(k)})$ for $k \in [1, \ell]$. Write $\chi := \sum_{k \in [1,\ell]} \chi_{(k)}$. Suppose the ordering to be chosen such that $\chi_{(1)} \leq \chi_{(2)} \leq \cdots \leq \chi_{(\ell)}$. Suppose that $h_{(k)}(X) \equiv_\pi X^{\chi_{(k)}}$ for $k \in [1, \ell]$. Write $\prod_{k \in [1,\ell]} h_{(k)}(X) =: \sum_{i \in [0,\chi]} b_i X^i$ with $b_i \in R$ for $i \in [0, \chi]$.*
Then $\mathrm{v}_\pi(b_i) \geq \ell - \max\{\, j \in [0, \ell] \,:\, \chi_{(1)} + \cdots + \chi_{(j)} \leq i \,\}$ for $i \in [0,\ \chi]$.

Proof. Write $h_{(k)}(X) =: \sum_{i \in [0,\chi_{(k)}]} h_{(k)i} X^i$ for $k \in [1, \ell]$, where $h_{(k)i} \in R$ for $i \in [0, \chi_{(k)}]$. We have $b_i = \sum_{i_{(k)} \in [0,\chi_{(k)}] \text{ for } k \in [1,\ell],\ i_{(1)}+\cdots+i_{(\ell)} = i} \prod_{k \in [1,\ell]} h_{(k)i_{(k)}}$. So it suffices to show that $\mathrm{v}_\pi\big(\prod_{k \in [1,\ell]} h_{(k)i_{(k)}}\big) \overset{!}{\geq} \ell - \max\{\, j \in [0, \ell] \,:\, \chi_{(1)} + \cdots + \chi_{(j)} \leq i \,\}$ for all occurring summands. Since $\mathrm{v}_\pi(h_{(k)i_{(k)}}) \geq 1$ if $i_{(k)} \in [0, \chi_{(k)} - 1]$, it remains to show that for such a summand, we have $|\{\, k \in [1, \ell] \,:\, i_{(k)} = \chi_{(k)} \,\}| \overset{!}{\leq} \max\{\, j \in [0, \ell] \,:\, \chi_{(1)} + \cdots + \chi_{(j)} \leq i \,\}$.
Assume that $|\{\, k \in [1, \ell] \,:\, i_{(k)} = \chi_{(k)} \,\}| > \max\{\, j \in [0, \ell] \,:\, \chi_{(1)} + \cdots + \chi_{(j)} \leq i \,\}$. Write $H := \{\, k \in [1, \ell] \,:\, i_{(k)} = \chi_{(k)} \,\} \subseteq [1, \ell]$. Then $\ell \geq |H| > \max\{\, j \in [0, \ell] \,:\, \chi_{(1)} + \cdots + \chi_{(j)} \leq i \,\}$, whence $\chi_{(1)} + \cdots + \chi_{(|H|)} > i$. So, using $\chi_{(1)} \leq \chi_{(2)} \leq \cdots \leq \chi_{(\ell)}$, we get $i = i_{(1)} + \cdots + i_{(\ell)} = \big(\sum_{k \in H} i_{(k)}\big) + \big(\sum_{k \in [1,\ell] \smallsetminus H} i_{(k)}\big) \geq \sum_{k \in H} i_{(k)} = \sum_{k \in H} \chi_{(k)} \geq \sum_{k \in [1,|H|]} \chi_{(k)} > i$, $\lightning$. □

Lemma 16.

(1) *We have* $e' \geq 0$.

(2) *Suppose given* $y \in \pi^{e'} R^{1\times M}$. *Then there exists* $x \in R^{1\times M}$ *such that* $xA(g_{(1)}\,,\,\dots\,,\,g_{(n)}) = y$.

(3) *Suppose given* $u \geq e'$ *and* $x \in R^{1\times M}$ *such that* $xA(g_{(1)}\,,\,\dots\,,\,g_{(n)}) \in R^{1\times M}\pi^u$.
Then $x \in R^{1\times M}\pi^{u-e'}$.

Proof. Write $\prod\limits_{j\in[1,n]\smallsetminus\{k\}} g_{(j)}(X) \; =: \sum\limits_{i\in[0,M_{(k)}]} a_{(k)i}X^i$ for $k \in [1,n]$.
Suppose given $i \in [1,M]$. Write $d_i := (n-1) - \max\{\, j \in [0,n-1] \,:\, m_{(1)} + \cdots + m_{(j)} \leq i-1 \,\}$. Note that $d_\xi \geq d_\eta$ for $1 \leq \xi \leq \eta \leq M$. By Lemma 15, we have $\mathrm{v}_\pi(a_{(k)i-1}) \;\geq\; d_i$ for $k \in [1,n]$, since the sequence of degrees of the polynomials $g_{(j)}(X)$, with $g_{(k)}(X)$ omitted, is entrywise bounded below by the sequence of degrees of the polynomials $g_{(j)}(X)$, i.e. by the sequence of the $m_{(j)}$. It follows that $\mathrm{v}_\pi(a_{(k)\xi-1}) \;\geq\; d_\xi \;\geq\; d_i$ for $k \in [1,n]$ and $\xi \in [1,i]$. Hence π^{d_i} divides column number i of $A(g_{(1)}\,,\,\dots\,,\,g_{(n)})$; cf. Definition 1.

We have

$$\begin{array}{rl} d_2 + \cdots + d_M & = \; \sum_{i\in[2,M]} \big((n-1) - \max\{\, j \in [0,n-1] \,:\, m_{(1)} + \cdots + m_{(j)} \leq i-1 \,\}\big) \\ = & (M-1)(n-1) - \sum_{i\in[1,M-1]} \max\{\, j \in [0,n-1] \,:\, m_{(1)} + \cdots + m_{(j)} \leq i \,\} \\ = & (M-1)(n-1) - \sum_{j\in[1,n-1]} j \cdot |\, [\, m_{(1)} + \cdots + m_{(j)}\,,\, m_{(1)} + \cdots + m_{(j)} + m_{(j+1)} - 1\,]\,| \\ = & (M-1)(n-1) - \sum_{j\in[1,n-1]} j m_{(j+1)} \;=\; (M-1)(n-1) - \sum_{j\in[1,n]} (j-1)m_{(j)} \\ = & (M-1)(n-1) + M - \sum_{j\in[1,n]} j m_{(j)} \;=\; 1 + nM - n - \sum_{j\in[1,n]} j m_{(j)} \\ = & 1 + \sum_{j\in[1,n]} \big((n-j)m_{(j)} - 1\big) \;=\; \sum_{j\in[1,n-1]} \big((n-j)m_{(j)} - 1\big)\;, \end{array}$$

whence $\mathrm{v}_\pi(\det A(g_{(1)}\,,\,\dots\,,\,g_{(n)})) - (d_2 + \cdots + d_M) \;=\; e'$. So assertion (2) follows by Lemma 9.(3), assertion (3) follows by Lemma 10.(3); moreover, assertion (1) follows by Remark 8. □

Lemma 17.

(1) *There exist monic polynomials* $\tilde g_{(1)}(X), \dots, \tilde g_{(n)}(X) \in R[X]$ *such that*
$\tilde g_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *for* $k \in [1,n]$ *and* $f(X) \equiv_{\pi^{2(s-t')}} \prod\limits_{k\in[1,n]} \tilde g_{(k)}(X)$.

We call such a tuple $(\tilde g_{(k)}(X))_k$ *of polynomials an* admissible lift *of* $(g_{(k)}(X))_k$ *with respect to* s. *We have* $\mathrm{v}_\pi(\mathrm{Res}(\tilde g_{(1)}\,,\,\dots\,,\,\tilde g_{(n)})) = t$ *for any admissible lift* $(\tilde g_{(k)}(X))_k$ *of* $(g_{(k)}(X))_k$ *with respect to* s.

(2) *Suppose given* $r \in [0, s-2t']$. *Suppose given monic polynomials* $\tilde g_{(1)}(X)\,,\,\dots\,,\,\tilde g_{(n)}(X)$, $\tilde h_{(1)}(X), \dots, \tilde h_{(n)}(X) \in R[X]$ *such that* $\tilde g_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *and* $\tilde h_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *for* $k \in [1,n]$ *and* $\prod\limits_{k\in[1,n]} \tilde g_{(k)}(X) \equiv_{\pi^{2(s-t')-r}} \prod\limits_{k\in[1,n]} \tilde h_{(k)}(X)$. *Then* $\tilde g_{(k)}(X) \equiv_{\pi^{2s-3t'-r}} \tilde h_{(k)}(X)$ *for* $k \in [1,n]$.

In particular, considering the case $r = 0$, *two admissible lifts with respect to* s *as in* (1) *are mutually congruent modulo* $\pi^{2s-3t'}R[X]$.

In the following proof, we shall use the notation of § 1.

Proof. Ad (1). *Existence of admissible lift.* We make the ansatz $\tilde{g}_{(k)}(X) = g_{(k)}(X)+\pi^{s-t'}u_{(k)}(X)$ for $k \in [1,n]$ with $u_{(k)}(X) \in R[X]$ and $\deg u_{(k)} < \deg g_{(k)} = m_{(k)}$ for $k \in [1,n]$. Thus we require that

$$\begin{aligned} f(X) \;&\overset{!}{\equiv}_{\pi^{2(s-t')}}\; \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \;=\; \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t'}u_{(k)}(X)) \\ &\equiv_{\pi^{2(s-t')}}\; \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t'} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,. \end{aligned}$$

Let $b(X) := \pi^{t'-s}(f(X) - \prod_{k\in[1,n]} g_{(k)}(X))$. Since $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$, we get $b(X) \equiv_{\pi^{t'}} 0$. So our requirement reads $b(X) \overset{!}{\equiv}_{\pi^{s-t'}} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,$. So it suffices to find $u_{(k)}(X) \in R[X]$ for $k \in [1,n]$ as above such that $b(X) \overset{!}{=} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,$.

Writing $b(X) =: \sum_{i\geq 0} \beta_i X^i$, $\prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) =: \sum_{i\geq 0} a_{(k)i}X^i$, $u_{(k)}(X) =: \sum_{i\geq 0} u_{(k)i}X^i$ for $k \in [1,n]$, where $\beta_i\,,\ a_{(k)i}\,,\ u_{(k)i} \in R$ for $i \geq 0$, a comparison of coefficients shows that it suffices to find

$$U \;:=\; (\underbrace{u_{(1)\,0}\;\dots\;u_{(1)\,m_{(1)}-1}}_{}\;\underbrace{u_{(2)\,0}\;\dots\;u_{(2)\,m_{(2)}-1}}_{}\;\;\dots\;\;\underbrace{u_{(n)\,0}\;\dots\;u_{(n)\,m_{(n)}-1}}_{}) \;\in\; R^{1\times M}$$

such that $U \cdot A(g_{(1)}\,,\,\dots\,,\,g_{(n)}) \;\overset{!}{=}\; (\beta_0\;\dots\;\beta_{M-1})$. Note that $(\beta_0\;\dots\;\beta_{M-1}) \in \pi^{t'}R^{1\times M}$ since $b(X) \equiv_{\pi^{t'}} 0$. So U exists as required by Lemma 16.(2).

Valuation of resultant. Since $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k \in [1,n]$, Remark 7 implies that $\mathrm{Res}(\tilde{g}_{(1)},\dots,\tilde{g}_{(n)}) \equiv_{\pi^{s-t'}} \mathrm{Res}(g_{(1)},\dots,g_{(n)})\,$. Since $s - t' \geq t+1 = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\dots\,,\,g_{(n)}))+1$, this implies $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}\,,\,\dots\,,\,\tilde{g}_{(n)})) \;=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\dots\,,\,g_{(n)})) \;=\; t\,$.

Ad (2). Writing $\tilde{g}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t'}u_{(k)}(X)$ and $\tilde{h}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t'}v_{(k)}(X)$ for $k \in [1,n]$, where $u_{(k)}(X),\ v_{(k)}(X) \in R[X]$, we obtain $\deg u_{(k)}(X) < \deg g_{(k)}(X) = m_{(k)}\,$, since $\tilde{g}_{(k)}(X)$ and $g_{(k)}(X)$ are monic polynomials of the same degree; likewise, we obtain $\deg v_{(k)}(X) < m_{(k)}\,$.

We have to show that $u_{(k)}(X) \overset{!}{\equiv}_{\pi^{s-2t'-r}} v_{(k)}(X)$ for $k \in [1,n]$. We have

$$\begin{aligned} &\prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t'} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \;\equiv_{\pi^{2(s-t')}}\; \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t'}u_{(k)}(X)) \\ &\qquad = \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \;\equiv_{\pi^{2(s-t')-r}}\; \prod_{k\in[1,n]} \tilde{h}_{(k)}(X) \\ &= \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t'}v_{(k)}(X)) \;\equiv_{\pi^{2(s-t')}}\; \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t'} \sum_{k\in[1,n]} v_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,. \end{aligned}$$

The difference yields $\sum_{k\in[1,n]} (u_{(k)}(X) - v_{(k)}(X)) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \;\equiv_{\pi^{s-t'-r}}\; 0\,$.

Writing $w_{(k)}(X) \;:=\; u_{(k)}(X) - v_{(k)}(X)$ for $k \in [1,n]$, this reads

$$(*) \qquad \sum_{k\in[1,n]} w_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \;\equiv_{\pi^{s-t'-r}}\; 0\,.$$

Writing $w_{(k)}(X) \;=:\; \sum_{i\geq 0} w_{(k)i}X^i$ for $k \in [1,n]$, and

$$W \;:=\; (\underbrace{w_{(1)\,0}\;\dots\;w_{(1)\,m_{(1)}-1}}_{}\;\underbrace{w_{(2)\,0}\;\dots\;w_{(2)\,m_{(2)}-1}}_{}\;\;\dots\;\;\underbrace{w_{(n)\,0}\;\dots\;w_{(n)\,m_{(n)}-1}}_{}) \;\in\; R^{1\times M}\;,$$

we have to show that $W \overset{!}{\in} \pi^{s-2t'-r} R^{1\times M}$. From $(*)$, we obtain $W \cdot A(g_{(1)}, \ldots, g_{(n)}) \in \pi^{s-t'-r} R^{1\times M}$. Note that $s - t' - r \geq t' = e'$. So we can infer by Lemma 16.(3) that $W \in \pi^{(s-t'-r)-t'} R^{1\times M} = \pi^{s-2t'-r} R^{1\times M}$. $\square$

Theorem 18. *Suppose R to be complete.*

Then there exist unique monic polynomials $\check{g}_{(1)}(X), \ldots, \check{g}_{(n)}(X) \in R[X]$ such that $\check{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k \in [1,n]$ and $f(X) = \prod\limits_{k\in[1,n]} \check{g}_{(k)}(X)$.

Proof. Existence. Since R is complete, it suffices to show that there exist monic polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ such that $f(X) \equiv_{\pi^{s+1}} \prod\limits_{k\in[1,n]} \tilde{g}_{(k)}(X)$ and $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k \in [1,n]$, and $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})) = t$. This follows from Lemma 17.(1) since $2(s-t') \geq s+1$.

Uniqueness. Given $\check{g}_{(1)}(X), \ldots, \check{g}_{(n)}(X)$, $\check{h}_{(1)}(X), \ldots, \check{h}_{(n)}(X) \in R[X]$, all monic, such that $\check{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X) \equiv_{\pi^{s-t'}} \check{h}_{(k)}(X)$ for $k \in [1,n]$ and $\prod\limits_{k\in[1,n]} \check{g}_{(k)}(X) = f(X) = \prod\limits_{k\in[1,n]} \check{h}_{(k)}(X)$, we have to show that $\check{g}_{(k)}(X) \overset{!}{=} \check{h}_{(k)}(X)$ for $k \in [1,n]$.

Note that $\mathrm{v}_\pi(\mathrm{Res}(\check{g}_{(1)}, \ldots, \check{g}_{(n)})) = t = \mathrm{v}_\pi(\mathrm{Res}(\check{h}_{(1)}, \ldots, \check{h}_{(n)}))$ by Lemma 17.(1).

Let $s_1 := s$. Both $(\check{h}_{(k)}(X))_k$ and $(\check{g}_{(k)}(X))_k$ are admissible lifts of $(\check{g}_{(k)}(X))_k$ with respect to s_1 in the sense of Lemma 17.(1), since $\check{h}_{(k)}(X) \equiv_{\pi^{s_1-t'}} \check{g}_{(k)}(X)$ for $k \in [1,n]$ and the other required congruences are verified using equalities. So Lemma 17.(2) yields $\check{h}_{(k)}(X) \equiv_{\pi^{2(s_1-t')-t'}} \check{g}_{(k)}(X)$ for $k \in [1,n]$.

Let $s_2 := 2(s_1 - t')$. Note that $s_2 = s_1 + (s_1 - 2t') > s_1$. Both $(\check{h}_{(k)}(X))_k$ and $(\check{g}_{(k)}(X))_k$ are admissible lifts of $(\check{g}_{(k)}(X))_k$ with respect to s_2, since $\check{h}_{(k)}(X) \equiv_{\pi^{s_2-t'}} \check{g}_{(k)}(X)$ for $k \in [1,n]$ So Lemma 17.(2) yields $\check{h}_{(k)}(X) \equiv_{\pi^{2(s_2-t')-t'}} \check{g}_{(k)}(X)$ for $k \in [1,n]$.

Let $s_3 := 2(s_2 - t')$. Note that $s_3 = s_2 + (s_2 - 2t') > s_2 + (s_1 - 2t') > s_2$. Continue as above.

This yields a strictly increasing sequence $(s_\ell)_{\ell\geq 1}$ of integers such that $\check{h}_{(k)}(X) \equiv_{\pi^{s_\ell-t'}} \check{g}_{(k)}(X)$ for $k \in [1,n]$ and $\ell \geq 1$. Hence $\check{h}_{(k)}(X) = \check{g}_{(k)}(X)$ for $k \in [1,n]$. $\square$

Example 19. Suppose that $n = 3$ and $s \geq 2t+1$. Write $t_0 := \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}, g_{(3)}))$ and $t_1 := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, g_{(2)}g_{(3)}))$. Lemma 2 gives $\mathrm{Res}(g_{(1)}, g_{(2)}, g_{(3)}) = \mathrm{Res}(g_{(1)}, g_{(2)}g_{(3)}) \cdot \mathrm{Res}(g_{(2)}, g_{(3)})$, whence $t = t_1 + t_0$. In particular, $\mathrm{Res}(g_{(1)}, g_{(2)}g_{(3)}) \neq 0$ and $\mathrm{Res}(g_{(2)}, g_{(3)}) \neq 0$.

Denote $t' := t - 2m_{(1)} - m_{(2)} + 2$, $t'_0 := t_0 - m_{(2)} + 1$ and $t'_1 := t_1 - m_{(1)} + 1$. So $s \geq 2t+1 \geq t+t'+1$ and $t' = t'_1 + t'_0 - m_{(1)}$.

We can apply Lemma 17.(1) to $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ to obtain monic polynomials $\tilde{g}_{(1)}(X)$, $\tilde{g}_{(2)}(X)$, $\tilde{g}_{(3)}(X) \in R[X]$ such that

(i′) $\quad \tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k \in [1,3]$, $\quad f(X) \equiv_{\pi^{2(s-t')}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) \cdot \tilde{g}_{(3)}(X)$.

We can also apply Lemma 17.(1) first to the factorisation $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot (g_{(2)}(X) \cdot g_{(3)}(X))$ and then to the resulting factorisation of the second factor into $g_{(2)}(X) \cdot g_{(3)}(X)$ modulo a certain power of π.

We have $s \geq 2t+1 \geq 2t_1+1 \geq t_1 + t'_1 + 1$. So Lemma 17.(1) gives monic polynomials $\tilde{h}_{(1)}(X)$, $\tilde{h}_{(2)}(X) \in R[X]$ such that

$$\tilde{h}_{(1)}(X) \equiv_{\pi^{s-t'_1}} g_{(1)}(X)\,, \quad \tilde{h}_{(2)}(X) \equiv_{\pi^{s-t'_1}} g_{(2)}(X) \cdot g_{(3)}(X)\,, \quad f(X) \equiv_{\pi^{2(s-t'_1)}} \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X)\,.$$

We have $s \geq 2t{+}1 \geq 2t{-}m_{(2)}{-}m_{(1)}{+}3{-}t_1 = (2t_0{-}m_{(2)}{+}1){+}(t_1{-}m_{(1)}{+}1){+}1 = (t_0{+}t'_0){+}t'_1{+}1$ and thus $s{-}t'_1 \geq t_0{+}t'_0{+}1$. So Lemma 17.(1) gives monic polynomials $\tilde{\tilde{g}}_{(2)}(X)$, $\tilde{\tilde{g}}_{(3)}(X) \in R[X]$ such that

$$\begin{aligned} \tilde{\tilde{g}}_{(2)}(X) \;\equiv_{\pi^{(s-t'_1)-t'_0}}\; g_{(2)}(X)\,, \quad \tilde{\tilde{g}}_{(3)}(X) \;\equiv_{\pi^{(s-t'_1)-t'_0}}\; g_{(3)}(X)\,, \\ \tilde{h}_{(2)}(X) \;\equiv_{\pi^{2((s-t'_1)-t'_0)}}\; \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X)\,. \end{aligned}$$

Altogether, the two subsequent applications of Lemma 17.(1) for two factors yield

$$\text{(ii}'\text{)} \quad \begin{aligned} &\tilde{h}_{(1)}(X) \;\equiv_{\pi^{s-t'_1}}\; g_{(1)}(X)\,.\; \tilde{\tilde{g}}_{(2)}(X) \;\equiv_{\pi^{s-t'_1-t'_0}}\; g_{(2)}(X)\,,\; \tilde{\tilde{g}}_{(3)}(X) \;\equiv_{\pi^{s-t'_1-t'_0}}\; g_{(3)}(X) \\ &f(X) \;\equiv_{\pi^{2(s-t'_1)}}\; \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \;\equiv_{\pi^{2(s-t'_1-t'_0)}}\; \tilde{h}_{(1)}(X) \cdot \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X)\,. \end{aligned}$$

Comparing the result (i$'$) of Lemma 17.(1) for three factors with the result (ii$'$) of two subsequent applications of Lemma 17.(1) for two factors, the former method yields a precision of $s - t'$ for the factors and a precision of $2(s-t')$ for the product decomposition, the latter method yields a precision of $s{-}t'_0{-}t'_1$ for the factors and a precision of $2(s{-}t'_0{-}t'_1)$ for the product decomposition. Since $t' = t'_1 + t'_0 - m_{(1)} < t'_1 + t'_0$, the former method yields a higher precision.

3 Examples

To illustrate Theorem 12 we consider some polynomials in the complete discrete valuation ring $\mathbb{Z}_p$ for a prime number p. Given a polynomial in $\mathbb{Z}[X] \subseteq \mathbb{Z}_p[X]$ and a factor decomposition in $\mathbb{Z}[X]$ to a certain p-adic precision, the method of the proof of Lemma 11 gives a factor decomposition in $\mathbb{Z}[X]$ to a higher p-adic precision. We use the notation of Lemma 11.

Let s be the current precision. Write $g_{(k)}(X) =: \sum_{j \in [0, m_{(k)}]} c_{(k)j} X^j$ and $\tilde{g}_{(k)}(X) =: \sum_{j \in [0, m_{(k)}]} \tilde{c}_{(k)j} X^j$ for $k \in [1, n]$, where $c_{(k)j}$, $\tilde{c}_{(k)j} \in \mathbb{Z}$. Write

$$s' \;:=\; \min\,\{\, \mathrm{v}_\pi(c_{(k)j} - \tilde{c}_{(k)j}) \;:\; k \in [1,n],\, j \in [0, m_{(k)}] \,\}\,.$$

By Lemma 11, we have $s' \geq s - t$. Let the *defect* be $s - s'$. The defect is bounded above by t.

If $f(X) \equiv_\pi X^M$ and the degrees of the factors $g_{(k)}(X)$ are sorted increasingly, then the defect $s - s'$ is bounded above by t'; cf. Lemma 17.

The following examples have been calculated using Magma [**1**].

Example 20. We consider the polynomial

$$f(X) = X^3 + X^2 - 2X + 8$$

at $p = 2$. This polynomial is also used as an example in [**5,** §3.12, Einleitung zu §4, §4.4].

We start with initial precision $s = 3$. We consider the development of the factors $g_{(1)}(X)$, $g_{(2)}(X)$, $g_{(3)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X$ $g_{(2)}(X) = X + 2$ $g_{(3)}(X) = X + 7$
step 2	$g_{(1)}(X) = X + 12$ $g_{(2)}(X) = X + 14$ $g_{(3)}(X) = X + 7$
step 3	$g_{(1)}(X) = X + 52$ $g_{(2)}(X) = X + 54$ $g_{(3)}(X) = X + 23$
step 4	$g_{(1)}(X) = X + 980$ $g_{(2)}(X) = X + 470$ $g_{(3)}(X) = X + 599$
step 5	$g_{(1)}(X) = X + 167380$ $g_{(2)}(X) = X + 224214$ $g_{(3)}(X) = X + 132695$
step 6	$g_{(1)}(X) = X + 1339592148$ $g_{(2)}(X) = X - 4836725802$ $g_{(3)}(X) = X + 3497133655$

We obtain the following results in the first 10 steps. The defect is bounded above by $t = 1$.

step	current precision s	defect $s - s'$
1	3	1
2	4	1
3	6	1
4	10	1
5	18	1
6	34	1
7	66	1
8	130	1
9	258	1
10	514	1

The defect seems to be constant with value 1. We observe that the defect is maximal. Note that in step 1, the precision grows only by 1.

Example 21.

We consider the polynomial

$$f(X) \;=\; X^8 + 3072X^2 + 16384$$

at $p = 2$. We start with initial precision $s = 103$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 48068350242001649882035977724980 \\ g_{(2)}(X) &= X - 48068350242001649882035977724980 \\ g_{(3)}(X) &= X^6 - 1093062124198142780466248559984X^4 \\ &\quad -4943636030726675686411786481408X^2 \\ &\quad -4341143474460317541052331090944. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t = 23$. Since $f(X) \equiv_2 X^8$, the defect is even bounded above by $t' = 22$.

step	current precision s	defect $s - s'$
1	103	3
2	200	4
3	392	5
4	774	1
5	1546	9
6	3074	3
7	6142	7
8	12270	3
9	24534	7
10	49054	3

Example 22.

We consider the polynomial

$$f(X) = X^{10} + 54X - 243$$

at $p = 3$. We start with initial precision $s = 46$, for which we have the initial factorisation into the factors

$$\begin{array}{rcl} g_{(1)}(X) & = & X + 1254845291302170687078 \\ g_{(2)}(X) & = & X^3 + 3439114880299728595329X^2 \\ & & +2097912255269159518284X \\ & & +2387878303991212496958 \\ g_{(3)}(X) & = & X^6 + 4168977948050601813522X^5 \\ & & +3414335924445189447372X^4 \\ & & -4695237998019536297 10X^3 \\ & & -3733781694469525960542X^2 \\ & & +2741122263554615006433X \\ & & +3057293995913895085035. \end{array}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t = 13$. Since $f(X) \equiv_3 X^{10}$, the defect is even bounded above by $t' = 10$.

step	current precision s	defect $s - s'$
1	46	3
2	86	0
3	172	3
4	338	2
5	672	1
6	1342	2
7	2680	1
8	5358	2
9	10712	1
10	21422	2

The defect seems to be eventually periodic.

References

[1] Bosma, W.; Cannon, J.J.; Fieker, C.; Steel, A. (eds.), *Handbook of Magma functions,* Edition 2.16, 2010; cf. magma.maths.usyd.edu.au.

[2] Frei, G., *The Unpublished Section Eight: On the Way to Function Fields over a Finite Field,* in: The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae, Springer, 2007.

[3] Gauss, C.F., *Werke,* Band II, zweiter Abdruck, 1876.

[4] Hensel, K., *Neue Grundlagen der Arithmetik,* J. Reine Angew. Math. 127, p. 51–84, 1904.

[5] Koch, H., *Zahlentheorie,* Vieweg, 1997.

[6] van der Waerden, B. L., *Algebra,* Springer Grundlehren, 5. Aufl., 1960.

Juliane Deißler
University of Stuttgart
Fachbereich Mathematik
Pfaffenwaldring 57
D-70569 Stuttgart
deissljе@stud.mathematik.uni-stuttgart.de